SPECIFICATION AMENDMENTS

Please replace paragraph [0053] with the following amended paragraph:

[0053] Figure 4 shows a flowchart corresponding to one embodiment of a mechanism for performing trusted firmware processes during OS-runtime. It will be understood that the initialization operations of Figure 2 or similar operations will have been performed during the pre-boot prior to booting and operating system and entering the OS-runtime phase. The process starts with an SMI or PMI event in a block 400. In response, the current SMM or PMI startup code is measured in a block 402. This measurement is analogous to the measurements performed in blocks 212 and 222 of Figure 2. Prior to this measurement, the SMM or PMI startup code is deemed "unqualified." This is because there is no way to verify whether the current SMM or PMI startup code is trustworthy or not without some sort of qualification, such as the measurement performed in block 402.

Please replace paragraph [0057] with the following amended paragraph:

[0057] There are many ~~advantageous~~ advantages to being able to operate in a locality above locality 0. A principle advantage concerns storing security and authentication data. These type of data are generally referred to as "secrets," and include such objects as keys and authentication certificates. The embodiments described below employ both physical mechanisms and logical mechanisms to prevent unauthorized access to such secrets.